

Commissioners:
T. JAMES DAVIS
LYNN M. HEMINGER
RONALD E. SKAGEN

General Manager:
WILLIAM C. DOBBINS



Public Utility District No. 1 of Douglas County

1151 Valley Mall Parkway • East Wenatchee, Washington 98802-4497 • 509/884-7191 • FAX 509/884-0553 • www.douglas pud.org

Received & Inspected

March 12, 2010

APR - 8 2010

FCC Mail Room

Ms. Marlene H. Dortch
Secretary of the Federal Communications Commission
445 12th Street SW
Washington, DC 20554

**Re: Public Utility District No. 1 of Douglas County, Washington
System Security and Integrity Plan
ET Docket No. 04-295**

Dear Ms. Dortch:

Enclosed, pursuant to 47 C.F.R. §1.20005, please find an original and four copies of the following documents:

- 1) System Security and Integrity Plan for Public Utility District No. 1 of Douglas County, Washington ("Douglas County PUD"); and
- 2) Appendix A to the System Security and Integrity Plan for Douglas County PUD.

Previously, Douglas County PUD enlisted the services of a Trusted Third Party in relation to CALEA compliance. Douglas County PUD will no longer be utilizing this Trusted Third Party. As such, it is submitting the enclosed documents as an update to its prior filings, primarily regarding its "24/7" contact information.

Thank you for your time and assistance.

Sincerely,

William C. Dobbins
General Manager

Enclosures

cc: Mr. David Ward, Senior Legal Advisor, Policy Division, Public Safety and Homeland Security Bureau, FCC

No. of Copies rec'd 0+4
List ABCDE

SYSTEM SECURITY AND INTEGRITY PLAN FOR PUBLIC UTILITY DISTRICT NO. 1 OF DOUGLAS COUNTY, WASHINGTON

Regulations of the Federal Communications Commission (FCC) require Public Utility District No. 1 of Douglas County, Washington (hereinafter "Douglas County PUD") to prepare and file a System Security and Integrity Plan, intended to ensure that any interception of communications or access to call-identifying information occurring within Douglas County PUD's network and premises, complies with legal requirements of the FCC and other applicable law. Specifically, this document shall ensure that such interception is activated only in accordance with appropriate legal authorization, appropriate carrier authorization, and with affirmative intervention and approval of an individual officer or employee of Douglas County PUD, acting in accordance with regulations prescribed by the Commission.

I. GENERAL OBLIGATIONS OF PERSONNEL

Any employee that receives a request from a law enforcement agency or anyone else for any form of electronic surveillance must follow these procedures exactly. Failure to adhere to the procedures set forth herein may result in disciplinary action, including possible termination of employment.

Any employee who receives a request for any form of electronic surveillance or request for call-identifying data, whether from a law enforcement official or from any other person, shall immediately direct the requesting party to Gary Ivory, Douglas County PUD Assistant General Manager, Customer Service, who has been designated by Douglas County PUD as the System Security and Integrity Plan Representative (hereinafter "SSI Representative"). The SSI Representative is the person authorized to accept these requests to Douglas County PUD and to act upon them and further, shall serve as the point of contact for law enforcement concerning a court-ordered surveillance request twenty-four hours a day, seven days a week. Full contact information for the SSI Representative is included in *Appendix A*, attached hereto and incorporated herein by reference.

The SSI Representative is specifically charged with the responsibility to assist law enforcement in conducting any interception of communications or providing access to call-identifying information. In the event that the SSI Representative is not available, all requests must be immediately directed to the most senior management employee available.

II. APPROPRIATE LEGAL AUTHORIZATION

Gary Ivory, the SSI Representative, is responsible for ensuring that appropriate legal authorization is provided prior to granting carrier authorization for an interception or access to call-identifying data. Such authority may consist of a court order signed by a judge or a magistrate authorizing or approving interception of wire or electronic

communications, or other authorization pursuant to 18 U.S.C. §2518(7), or any other relevant federal or state statute providing affirmative legal authority for such action.

III. CERTIFICATION AND RECORDS RETENTION

Information regarding each interception of communication or access to call-identifying data, whether authorized or not, will be documented and securely maintained in the form of a single certificate. This certificate must include, at a minimum:

- (i) The identity of the law enforcement officer presenting the authorization, including his/her name, agency and department;
- (ii) The name of the person signing the appropriate legal authorization, along with a copy of the court order or equivalent authorization or, in the case of an unauthorized interception, all available documentation detailing the request;
- (iii) Information regarding the surveillance request, including: the date and time it was presented; the date and time of implementation; and the type of interception of communications or access to call-identifying information requested (e.g., pen register, trap and trace, Title III, FISA);
- (iv) The telephone number(s) and/or circuit identification numbers involved;
- (v) The start date and time that the carrier enables the interception of communications or access to call-identifying information and the duration of the interception;
- (vi) The actions taken to obtain this information; and
- (vii) The name, title and signature of the SSI Representative authorizing and overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carrier's policies established under 47 C.F.R. §64.2103.

The certificate will be compiled either contemporaneously with, or within a reasonable period of time after, the initiation of the interception of communications or access to call-identifying data, or the unauthorized request.

After review of the certification form and associated documents, the SSI Representative will sign and date the record, certifying that it is complete and accurate. Additionally, the SSI Representative will ensure that the records are maintained securely for no less than two (2) calendar years.

//

//

//

//


IV. UNAUTHORIZED USE OF SURVEILLANCE CAPABILITIES

Any employee who knowingly misuses intercept capabilities intended for lawful surveillance will face disciplinary measures, up to and including dismissal.

Information regarding any act or attempted act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities, and any act of unauthorized electronic surveillance, will be reported to local law enforcement within a reasonable time upon discovery.

These policies and procedures will remain in effect until notice is provided to the Commission regarding a significant change.

Signed this 29 of March, 2010.



Mr. William C. Dobbins
General Manager

APPENDIX A
to
SYSTEM SECURITY AND INTEGRITY PLAN
for Public Utility District No. 1 of Douglas County, Washington

SSI Representative

Name/Title:	Mr. Gary Ivory Public Utility District No. 1 of Douglas County, Washington, Assistant Manager, Customer Service
Phone:	509-881-7191
Cellular:	509-630-0676
Email for Requests:	<u>GaryI@dcpud.org</u>

SYSTEM SECURITY AND INTEGRITY PLAN FOR PUBLIC UTILITY DISTRICT NO. 1 OF DOUGLAS COUNTY, WASHINGTON

Regulations of the Federal Communications Commission (FCC) require Public Utility District No. 1 of Douglas County, Washington (hereinafter "Douglas County PUD") to prepare and file a System Security and Integrity Plan, intended to ensure that any interception of communications or access to call-identifying information occurring within Douglas County PUD's network and premises, complies with legal requirements of the FCC and other applicable law. Specifically, this document shall ensure that such interception is activated only in accordance with appropriate legal authorization, appropriate carrier authorization, and with affirmative intervention and approval of an individual officer or employee of Douglas County PUD, acting in accordance with regulations prescribed by the Commission.

I. GENERAL OBLIGATIONS OF PERSONNEL

Any employee that receives a request from a law enforcement agency or anyone else for any form of electronic surveillance must follow these procedures exactly. Failure to adhere to the procedures set forth herein may result in disciplinary action, including possible termination of employment.

Any employee who receives a request for any form of electronic surveillance or request for call-identifying data, whether from a law enforcement official or from any other person, shall immediately direct the requesting party to Gary Ivory, Douglas County PUD Assistant General Manager, Customer Service, who has been designated by Douglas County PUD as the System Security and Integrity Plan Representative (hereinafter "SSI Representative"). The SSI Representative is the person authorized to accept these requests to Douglas County PUD and to act upon them and further, shall serve as the point of contact for law enforcement concerning a court-ordered surveillance request twenty-four hours a day, seven days a week. Full contact information for the SSI Representative is included in *Appendix A*, attached hereto and incorporated herein by reference.

The SSI Representative is specifically charged with the responsibility to assist law enforcement in conducting any interception of communications or providing access to call-identifying information. In the event that the SSI Representative is not available, all requests must be immediately directed to the most senior management employee available.

II. APPROPRIATE LEGAL AUTHORIZATION

Gary Ivory, the SSI Representative, is responsible for ensuring that appropriate legal authorization is provided prior to granting carrier authorization for an interception or access to call-identifying data. Such authority may consist of a court order signed by a judge or a magistrate authorizing or approving interception of wire or electronic

communications, or other authorization pursuant to 18 U.S.C. §2518(7), or any other relevant federal or state statute providing affirmative legal authority for such action.

III. CERTIFICATION AND RECORDS RETENTION

Information regarding each interception of communication or access to call-identifying data, whether authorized or not, will be documented and securely maintained in the form of a single certificate. This certificate must include, at a minimum:

- (i) The identity of the law enforcement officer presenting the authorization, including his/her name, agency and department;
- (ii) The name of the person signing the appropriate legal authorization, along with a copy of the court order or equivalent authorization or, in the case of an unauthorized interception, all available documentation detailing the request;
- (iii) Information regarding the surveillance request, including: the date and time it was presented; the date and time of implementation; and the type of interception of communications or access to call-identifying information requested (e.g., pen register, trap and trace, Title III, FISA);
- (iv) The telephone number(s) and/or circuit identification numbers involved;
- (v) The start date and time that the carrier enables the interception of communications or access to call-identifying information and the duration of the interception;
- (vi) The actions taken to obtain this information; and
- (vii) The name, title and signature of the SSI Representative authorizing and overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carrier's policies established under 47 C.F.R. §64.2103.

The certificate will be compiled either contemporaneously with, or within a reasonable period of time after, the initiation of the interception of communications or access to call-identifying data, or the unauthorized request.

After review of the certification form and associated documents, the SSI Representative will sign and date the record, certifying that it is complete and accurate. Additionally, the SSI Representative will ensure that the records are maintained securely for no less than two (2) calendar years.

//

//

//

//

IV. UNAUTHORIZED USE OF SURVEILLANCE CAPABILITIES

Any employee who knowingly misuses intercept capabilities intended for lawful surveillance will face disciplinary measures, up to and including dismissal.

Information regarding any act or attempted act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities, and any act of unauthorized electronic surveillance, will be reported to local law enforcement within a reasonable time upon discovery.

These policies and procedures will remain in effect until notice is provided to the Commission regarding a significant change.

Signed this 29 of March, 2010.

A handwritten signature in black ink, appearing to read "W C Dobbins", written over a horizontal line.

Mr. William C. Dobbins
General Manager

APPENDIX A
to
SYSTEM SECURITY AND INTEGRITY PLAN
for Public Utility District No. 1 of Douglas County, Washington

SSI Representative

Name/Title:	Mr. Gary Ivory Public Utility District No. 1 of Douglas County, Washington, Assistant Manager, Customer Service
Phone:	509-881-7191
Cellular:	509-630-0676
Email for Requests:	<u>GaryI@dcpud.org</u>